

# Arab Academy for Science, Technology, and Maritime Transport

## College of Computing and Information Technology

### IS703 Information Systems Security

### CS716 Data Security

Spring 2014

#### Homework 1 (Total of 50 pts) Due in class on April 8<sup>th</sup> 2014

Please provide a softcopy of your homework (Always keep a copy of the homework you hand in). Page numbers refer to the 6<sup>th</sup> edition of the course textbook

**Q1:** (15 pts) Write a program (in any programming language) that would reproduce figure 2.3 on page 55 for the Caesar Cipher. Your program should accept as input the ciphertext and produce a tabular listing of all possible plaintexts. Provide the opposite functionality, i.e., given the plaintext, produce all possible ciphertexts for all key values. Test your program against the following two ciphertexts.

BZDRZQ'R VHED LTRS AD ZANUD RTROHBHNM  
KENKMOG PYBDEXK TEFKD

(ciphertexts obtained from <http://simonsingh.net/cryptography/cryptograms/>)

**Q2.** (15 pts) Provide a summary of the paper [\*Steganography: Seeing the Unseen\*](#) by [Neil F. Johnson](#) and [Sushil Jajodia](#). *IEEE Computer*, February 1998: 26-34. (The paper can be retrieved at <http://www.jjtc.com/pub/r2026.pdf>).

Locate and download one of the freely available software packages and attempt to use it to provide steganographic services. Provide a report detailing your experiences and the overall applied process.

**Q3. (20 pts)** Implement the *Vigenere* (polyalphabetic) cipher (in any programming language). Test encryption and decryption operations attempting different keyword options including the keyword *deceptive*)